EXHIBIT B

AO 106 (Rev. 01/09) Application for a Search Warrant

United States District Court

for the
Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

One (1) Apple iPhone 11 Pro, green in color, and bearing IMEI: 353248101165460, seized by law enforcement on February 28, 2021 (hereinafter referred to as the "**Subject Phone**").

Case No. 21-mj-22
(Filed Under Seal)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See description of Subject Phone, which is included in **Attachment A**, which is attached and incorporated by reference as though set forth fully herein

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See **Attachment B**, which is attached hereto and incorporated herein by reference as though set forth fully herein.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of 21 U.S.C. §§ 856 and 846 and 18 U.S.C. §§ 371, 201(b)(1), and 1594(c).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

CURTIS E RYAN Digitally signed by CURTIS E RYAN Date: 2021.03.11 16:45:07 -05'00'

Applicant's signature

CURTIS E. RYAN
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
Printed name and title

Sworn to before me and signed telephonically.
Date: March 12, 2021

Judge's signature

City and state: Buffalo, New York

HONORABLE H. KENNETH SCHROEDER, JR.
UNITED STATES MAGISTRATE JUDGE
Printed name and Title

AFFIDAVIT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, **CURTIS E. RYAN**, Special Agent of Homeland Security Investigations, United States Department of Homeland Security, having been duly sworn, states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of Homeland Security Investigations ("HSI") of the United States Department of Homeland Security. As such, I am an "investigative or law enforcement officer of the United States" within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

2. I have been employed as a Special Agent ("SA") with HSI since February of 2012. Prior to my employment with HSI, I served a Special Agent within the Department of Defense and the Department of Justice. I have been a Special Agent since April of 1999. During my career as a Special Agent, I have participated in investigations concerning terrorism, fraud, violent crimes, and drug trafficking. My investigative experience, as well as the experience of other law enforcement agents and officers who are participating in this investigation, serves as the basis for the opinions and conclusions set forth herein.

3. This affidavit is being submitted for a limited purpose, that is, to establish probable cause. Therefore, I have not presented all the information known to the United States. I have set forth only the information I believe is necessary to establish probable cause. The facts and conclusions set forth in this affidavit come from my personal observations, my training and experience, and information obtained from law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this manner.

4. Your affiant makes this affidavit in support of a federal search warrant application for the following cellular telephone and any applicable subscriber identity modules or subscriber identification modules ("SIM"), widely known as a SIM cards, all of which law enforcement recovered during the seized during the arrest of **PETER GERACE, JR.** on February 28, 2021, in the Southern District of Florida:

a. One (1) Apple iPhone 11 Pro, green in color, and bearing IMEI: 353248101165460, seized by law enforcement on February 28, 2021 (hereinafter referred to as the "**Subject Phone**"). See Attachment A, which is incorporated by reference as though set forth fully herein.

5. The **Subject Phone** is currently in the custody of HSI, located at 250 Delaware Avenue, Buffalo, New York.

6. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the Subject Phone is evidence of, was used in committing, and/or contains evidence/fruits/instrumentalities of:

- Conspiracy to Defraud the Government, in violation of Title 18, United States Code, Section 371;

- Paying a Bribe to a Public Official, in violation of Title 18, United States Code, Sections 201(b)(1)(A) and 201(b)(1)(C);

- Maintaining a Drug-Involved Premises, in violation of Title 21, United States Code, Section 856(a)(1) and Title 18, United States Code, Section 2;

- Conspiracy to Distribute Controlled Substances, in violation of Title 21, United States Code, Section 846; and,

- Conspiracy to Commit Sex Trafficking, in violation of Title 18, United States Code, Section 1594(c).

(hereinafter, the "Enumerated Offenses").

PROBABLE CAUSE

7. On November 29, 2019, your affiant applied for and received search warrants from this Court authorizing the search of 5145 Lexor Lane, Clarence, New York, and 999 Aero Drive, Cheektowaga, New York. See Case No. 19-MJ-5303 (see Attachment C). The search warrants authorized the search of the premises for the seizure of electronic devices, controlled substances, and other evidence. On December 12, 2019, law enforcement executed the search warrants at those premises. At that time, agents seized a small quantity of marijuana from 999 Aero Drive and recovered documentary evidence and electronic devices from both premises. During the execution of the search warrants, **PETER GERACE, JR.** was not present at either premises and law enforcement did not seize **GERACE's** mobile telephone.

8. On Thursday, February 25, 2021, a federal grand jury returned a Second Superseding Indictment against **PETER GERACE, JR.** and co-defendant Joseph Bongiovanni. See Case No. 19-CR-227. The Second Superseding Indictment contains 18

counts and four forfeiture allegations; the grand jury charged **GERACE** with five counts involving violations of the following:

- Conspiracy to Defraud the Government, in violation of Title 18, United States Code, Section 371;
- Paying a Bribe to a Public Official, in violation of Title 18, United States Code, Sections 201(b)(1)(A) and 201(b)(1)(C);
- Maintaining a Drug-Involved Premises, in violation of Title 21, United States Code, Section 856(a)(1) and Title 18, United States Code, Section 2;
- Conspiracy to Distribute Controlled Substances, in violation of Title 21, United States Code, Section 846; and,
- Conspiracy to Commit Sex Trafficking, in violation of Title 18, United States Code, Section 1594(c).

Following the return of the Second Superseding Indictment against **GERACE** and Bongiovanni, the Court issued an arrest warrant for the arrest of **GERACE** for the appearance of **GERACE** for the arraignment to be held before this Court.

9. On February 28, 2021, law enforcement arrested **PETER GERACE, JR.** in the Southern District of Florida and recovered his cellular phone from his person. On March 11, 2021, HSI Buffalo received the **Subject Phone** from law enforcement in Florida and it is currently in the custody of HSI, located at 250 Delaware Avenue, Buffalo, New York.

10. The investigation has shown that **PETER GERACE, JR.** used his mobile telephone to communicate with co-defendant Joseph Bongiovanni, and others, listed below in part:

a. Anthony Gerace, the younger brother of **PETER GERACE, JR.**, who on December 27, 2020, entered a plea of guilty to Count 7 of a Superseding Indictment which charged a violation of Title 18, United

States Code, Section 924(c)(1(a)(i) (possession of firearms in furtherance of drug trafficking. See Case No. 19-CR-86-JLS (MJR), Doc. No. 53 (see Attachment D).

b. [redacted]

c. [redacted]

d. [redacted]

11. Throughout the course of this investigation, agents have interviewed several witnesses regarding **PETER GERACE, JR.** use and distribution of controlled substances. Those witnesses have reported seeing **GERACE** use cocaine[1] and other controlled substances at his residence, that is, 5145 Lexor Lane, Clarence, New York, his business, that is, Pharaoh's Gentlemen's Club, located at 999 Aero Drive, Cheektowaga, New York, and elsewhere. Witnesses also reported receiving cocaine from **GERACE** and witnessing **GERACE** make cocaine available to others at 5145 Lexor Lane, Clarence, New York.

12. Your affiant believes evidence of the **PETER GERACE, JR.** involvement with the violations charged in the Second Superseding Indictment is presently stored in the Subject Phone. Based on my training and experience in conducting other investigations and my

[1] Cocaine is a Schedule II controlled substance.

discussions with other experienced law enforcement officers of HSI and DEA, I have learned the following:

a. Traffickers of controlled substances commonly maintain records, notes, and other papers relating to drug trafficking, some of which may be in code, including but not limited to sales receipts, shipping labels, shipping receipts, shipping boxes, order forms, storage receipts, records, operating manuals, computer records, publications, notes, checks, money orders, and money transfer receipts. The aforementioned records, notes, and other papers are commonly maintained where the smuggler or drug possessor/trafficker has ready access to them, such as on their person, or in their homes, garages, vehicles or businesses, or even in electronic storage devices, including, but not limited to computers, computer storage disks or drives, tablet devices, cellular telephones and other electronic devices.

b. Traffickers of controlled substances commonly maintain books or papers that reflect addresses or telephone numbers for their associates or sources of supply and such items may be in code. The above addresses and telephone numbers may also be stored in electronic storage mediums, including but not limited to cellular telephones, tablet devices, computers, computer storage disks or drives, and other electronic devices.

c. Traffickers of controlled substances commonly take, or cause to be taken, photographs/videos of themselves, their associates, their property, their drugs, or their proceeds, and usually maintain these photographs/videos in their residences. The above photographs/videos may also be stored in electronic storage media, including but not limited to, cellular telephones, digital cameras, tablet devices, home computers, computer storage disks or drives, and other electronic devices.

d. Cellular telephones frequently have telephone directory features, as well as methods to learn the telephone number associated with other cell phones. Cellular telephones also typically contain records of recent call activity, both incoming and outgoing calls, and lists of stored telephone numbers and other identifying information, such as names.

e. Cellular telephones typically have voice mail and/or text-messaging features, which permit the cellular telephone user to send and receive voice mail and/or text messages. Voice mail and text messages are typically stored on the computer network of the provider of the cell phone's telephone service, which network is external to the cell phone. Sent and received text messages may also be stored on the cell phone itself.

f. Cellular telephones with camera functions permit the cell phone user to take photographs and/or videos that are stored on the cell phone itself.

g. The information described in subparagraphs (g), (h) and (i) above, usually remains accessible in the cell phone's memory card even if the cell phone has lost all battery power, and not been used for an extended period of time.

h. Certain electronic devices, including i-Phones, Blackberries, i-Pods, and Android phones, store information such as email messages, chats, multimedia messages, installed applications or other electronic communications, calendars, notes, passwords, dictionary entries, Global Positioning Satellite (GPS) entries, internet protocol connections, and location entries, including cell tower and WiFi entries, and internet or browser entries or history. In addition, these devices often contain proprietary software, in the form of system, data, or configuration information, which enable the types of information and data described above to be accessed and analyzed. These items remained stored on the electronic devices even if the device in question has lost all battery power, and has not been used for an extended period of time.

13. Based on the foregoing facts and circumstances, there is probable cause to believe that the **Subject Phone**, recovered during the arrest of **PETER GERACE, JR.**, will contain evidence related to the Enumerated Offenses.

SUMMARY OF RELEVANT TECHNOLOGY

14. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "landline" telephones. A cellular telephone usually includes a "call log," which records the telephone number, date, and time of calls made to and from the phone. Each handheld wireless device is assigned a unique identifying number, known

as the international mobile equipment identity number ("IMEI") and/or the Electronic Serial Number ("ESN").

15. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device. Based on your affiant's training and experience, and the information learned throughout this investigation, persons associated with drug trafficking organizations utilize cellular telephones to communicate with others about the possession, transportation, and distribution of controlled substances, including cocaine.

16. According to research, a Secure Digital card ("SD card") is a non-volatile memory card designed for use in portable devices. Such cards are often used in, among other electronics, digital cameras, camcorders, video game consoles, and cellular phones. SD cards are manufactured with anywhere from 4 megabytes up to 2 terabytes of memory. The card's asymmetrical shaped sides prevent inserting it upside down.

SEEKING AUTHORIZATION TO SEARCH AND SEIZE

17. Based on my training, my experience, my participation in other narcotics investigations, my participation in this investigation, and my discussions with other

experienced law enforcement personnel, I have learned that significant narcotics traffickers such as dealers in cocaine and other controlled substances frequently maintain, in portable mobile communication and storage devices, addresses, email addresses and telephone numbers in directories, documents and files which reflect names, email addresses, addresses, telephone numbers, and objects related to drug trafficking, and photographs regarding drug trafficking and drug trafficking associates contained in the cellular telephones, as well as bank and other financial records. As it relates to the this case in particular, and based on my training and experience, cellular telephones and other communication and electronic devices will contain within their memory, contact lists, call logs, text messages, photos, videos, audio recordings, internet browser history, historical GPS locations and other information that would be pertinent to this ongoing investigation.

18. Based on my training, experience, and conversations with other law enforcement officers, individuals engaged in drug trafficking often possess multiple cellular phones. Drug traffickers and their co-conspirators commonly possess multiple cellular phones in an effort to wall off family and friends and avoid detection and identification by law enforcement.

19. Based on my training, my experience, my participation in other narcotics investigations, my participation in this investigation, and my discussions with other experienced law enforcement personnel, I have learned that significant narcotics traffickers, such as traffickers of controlled substances like cocaine, frequently maintain in portable mobile communication and storage devices incoming and outgoing calls and text messages, addresses, email addresses and telephone numbers in directories, documents and files which

reflect names, email addresses, addresses, telephone numbers, and objects related to drug trafficking, and photographs regarding drug trafficking and drug trafficking associates in their cellular telephones.

20. Accordingly, the application seeks authorization to search for and seize all:

a. lists of co-conspirators, counterparties, and customers, and related identifying information;

b. records of telephone calls, including incoming, outgoing, and missed calls, phone contact addresses, email addresses and telephone numbers in directories, documents and files which reflect names, email addresses, addresses, telephone numbers and objects related to paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking, and photographs regarding paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking and associates involved in paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking contained in the cellular telephones and SD cards;

c. text (SMS and MMS) messages and emails contained in the cellular telephones related to paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking;

d. applications used to communicate with individuals regarding paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking, including, but not limited to, Facebook, WhatsApp, Slack, Wickr, Snapchat;

e. all bank records, checks, credit card bills, account information, and other financial records; and,

f. records regarding the ownership and/or possession of the searched items.

21. Based on your Affiant's experience, it is believed the **Subject Phone** listed in **Attachment A** is evidence of and/or contain evidence of the Enumerated Offenses, which have been committed. Your affiant believes that evidence of the Enumerated Offenses, will be found in the **Subject Phone**. I submit there is probable cause to believe that **PETER GERACE, JR.** utilized this cellular device to contact other suppliers, customers, or co-conspirators regarding his involvement in narcotics and other violations, as charged in the Second Superseding Indictment. As such, I believe that the **Subject Phone** described above contains evidence of the Enumerated Offenses, which have been committed by **PETER GERACE, JR.** and others. The specific evidence in this regard is detailed in the Schedule of Items to Be Searched For and Seized listed in **Attachment B**, which is incorporated by reference as though set forth fully herein.

22. Based on your affiant's knowledge, training, and the experience of other agents with whom I have discussed this investigation, I know that in order to completely and accurately retrieve data maintained in cellular telephones hardware or software, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction, it is often necessary that the cellular telephones, related instructions in the form of manuals and notes, as well as the software utilized to operate such a device, be seized and subsequently processed by a qualified specialist in a laboratory setting.

ANALYSIS OF ELECTRONIC DATA

23. The search warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

24. Searching the cellular telephone for the evidence described above may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a cellular telephone for special words that are likely to appear only in the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Suspected criminals have the ability to mislabel or hide information and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the device's memory not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant.

25. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described above. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. There is probable cause to believe that things that were once stored on the **Subject Phone** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. Your affiant notes that due to the level of encryption that is anticipated on the **Subject Phone**, the process to extract the information from the phones may lead to the destruction of the phone.

28. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

FORENSIC EVIDENCE

29. As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each of the **Subject Phone** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Subject Phone** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Subject Phone** consistent with the warrants. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

MANNER OF EXECUTION

31. Because each warrant seeks only permission to examine a device already in law enforcement's possession, the execution of the warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

REQUEST TO SEAL

32. I further request Court order that all papers in support of this application, including the affidavit, attachments, and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and although efforts have been made to conceal their identity, provides information that could identify and potentially endanger the confidential sources referenced herein. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize this ongoing investigation.

WHEREFORE, based upon the foregoing, your affiant submits that there is probable cause to believe that the **Subject Phone** is evidence of, and/or contains evidence of, the Enumerated Offenses committed by **PETER GERACE Jr.** and/or evidence of the commission of the Enumerated Offenses by co-conspirators.

CURTIS E RYAN Digitally signed by CURTIS E RYAN Date: 2021.03.11 16:46:14 -05'00'

CURTIS E. RYAN
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me telephonically

this 12th day of March, 2021

H. Kenneth Schroeder

HONORABLE H. KENNETH SCHROEDER, JR.
United States Magistrate Judge

ATTACHMENT A

PROPERTY TO BE SEARCHED

SUBJECT PHONE

One (1) Apple iPhone 11 Pro, green in color, and bearing IMEI: 353248101165460, seized by law enforcement on February 28, 2021 (hereinafter referred to as the "**Subject Phone**").

ATTACHMENT B

SCHEDULE OF ITEMS TO BE SEARCHED FOR AND SEIZED

Items comprising evidence of, or property designed for use, intended for use, or used in committing violations of: Conspiracy to Defraud the Government, in violation of Title 18, United States Code, Section 371; Paying a Bribe to a Public Official, in violation of Title 18, United States Code, Sections 201(b)(1)(A) and 201(b)(1)(C); Maintaining a Drug-Involved Premises, in violation of Title 21, United States Code, Section 856(a)(1) and Title 18, United States Code, Section 2; Conspiracy to Distribute Controlled Substances, in violation of Title 21, United States Code, Section 846; and, Conspiracy to Commit Sex Trafficking, in violation of Title 18, United States Code, Section 1594(c):

a) lists of co-conspirators, counterparties, and customers, and related identifying information;

b) records of telephone calls, including incoming, outgoing, and missed calls, phone contact addresses, email addresses and telephone numbers in directories, documents and files which reflect names, email addresses, addresses, telephone numbers and objects related to paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking, and photographs regarding paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking and associates involved in paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking contained in the cellular telephones and SD cards;

c) text (SMS and MMS) messages and emails contained in the cellular telephones related to paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking;

d) applications used to communicate with individuals regarding paying a bribe to a public official, maintaining a drug-involved premises, conspiracy to distribute controlled substances, and conspiracy to commit sex trafficking, including, but not limited to, Facebook, WhatsApp, Slack, Wickr, Snapchat;

e) all bank records, checks, credit card bills, account information, and other financial records; and,

f) records regarding the ownership and/or possession of the searched item.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.